

ABSTRACT

A method and a circuit for masking digital data handled by an algorithm and factorized by a residue number system based on a finite base of numbers or polynomials prime to one another, comprising making the factorization base variable.